LAN-TSE Software

Inhaltsverzeichnis

Mit unserer Middleware steuern Sie einheitlich verschiedene TSE Geräte einfach an. Der Aufruf innerhalb des Netzwerkes erlaubt den einfachen Zugriff auf die TSE. Somit kann diese insbesondere auch aus Sicherheitsgründen (Diebstahl) z.B. im Server Rack installiert werden und muss nicht an der Kasse selbst installiert sein.

Download Link der Software:

https://www.dbfakt.de/downloads/get/54/dbfakt-lan-tse-software

Extrahieren der Dateien und erste Schritte

Bitte erstellen Sie einen neuen Ordner z.B.: c:\DBFAKT_TSE und kopieren danach die Dateien aus dem ZIP in den neuen Ordner.

Installation von

vc_redist.x64.exe

„Windows Powershell“ als Administrator aufrufen.

In den Ordner wechseln, wo die Dateien liegen:

cd c:\DBFAKT_TSE

.\lantse.ps1

Sollte nun eine Fehlermeldung kommen bzgl. etwaiger Berechtigungen, dann:

powershell-server-defaults.cmd

ausführen und Powershell neu starten.

Wenn immer noch Fehlermeldungen kommen wegen fehlender Benutzerrechte, dann:

Set-ExecutionPolicy RemoteSigned

und Powershell neu starten.

Konfiguration und Installation in der Konsole

Bei erster Installation bitte in nachfolgenden Reihenfolge starten:

.\lantse.ps1 config
.\lantse.ps1 install
.\lantse.ps1 add-eventlog
.\lantse.ps1 run

Wichtige Einstellungen der Config

.\lantse.ps1 config

Host	Entweder localhost / IP Adresse / oder * für beides
Port	z.B. 2020 (prüfen benutzter ports = „netstat -a -n | findstr ABH“)
PUK*²	123456
Admin Pin*²	12345
TimeAdmin-PIN*²	12345
Client-ID*²	dbFakt (dbFakt Nutzer zwingend „dbFakt“)
Laufwerk	Laufwerk der TSE z.B. „x“
AuthData	(Lizenzkey von dbFakt zum Aktivieren der Anwendung)

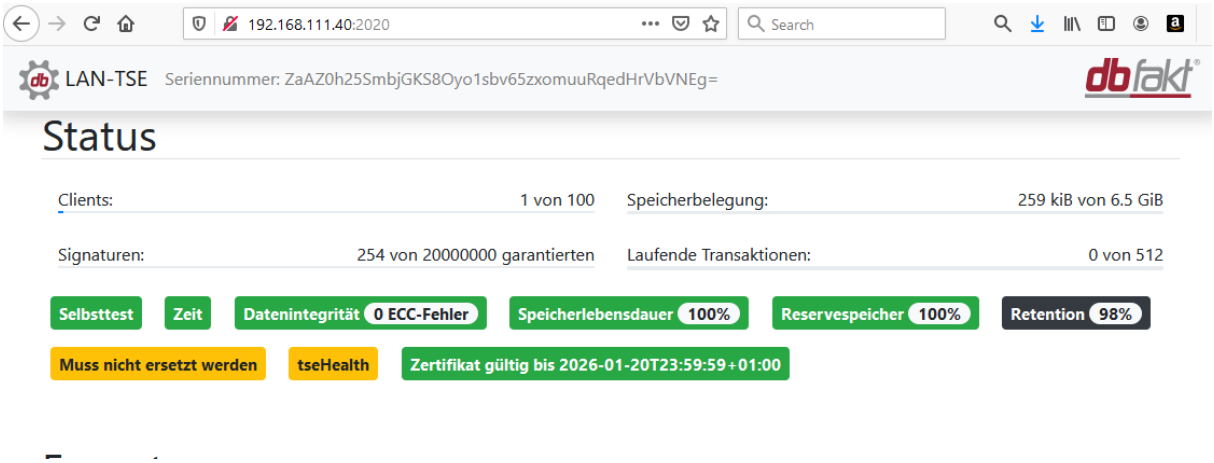
*² wird auf der TSE gespeichert

Install	Dienst installieren
Uninstall	Dienst entfernen
Start	Dienst starten
Stop	Dienst stoppen
Restart	Dienst neu starten
Add-Eventlog	Ereignisanzeige (bitte unbedingt aktivieren)
Del-Eventlog	Ereignisanzeige löschen
Get-Eventlog	Zeigt die 100 letzten Einträge in der Konsole an.
Run	Starten der Anwendung auf der Konsole

Weboberfläche nach erfolreich gestarteten Dienst

Rufen Sie bitte nach erfolgreicher Installation die Oberfläche über die in der Konfig eingegebene IP-Adresse und Port auf:

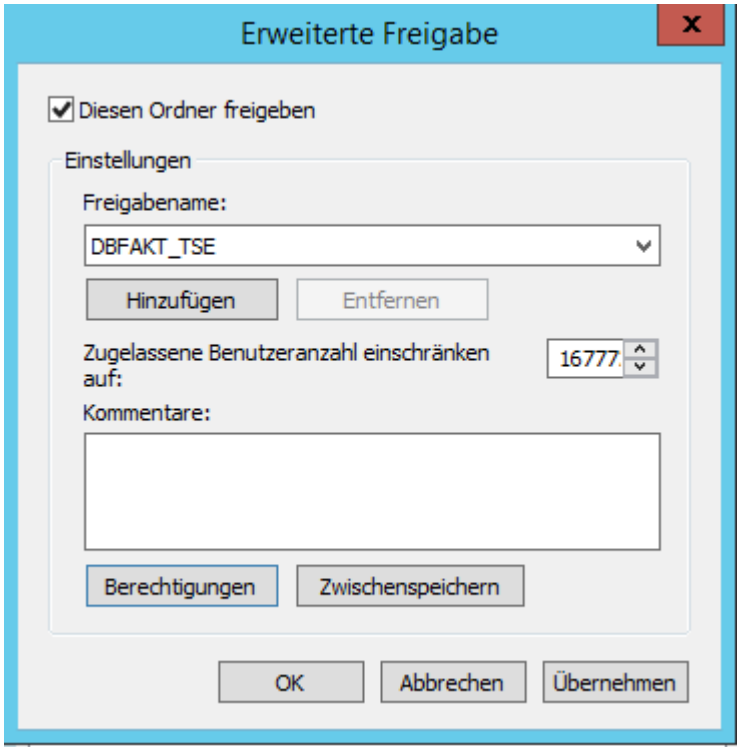
http://192.168.111.40:2020



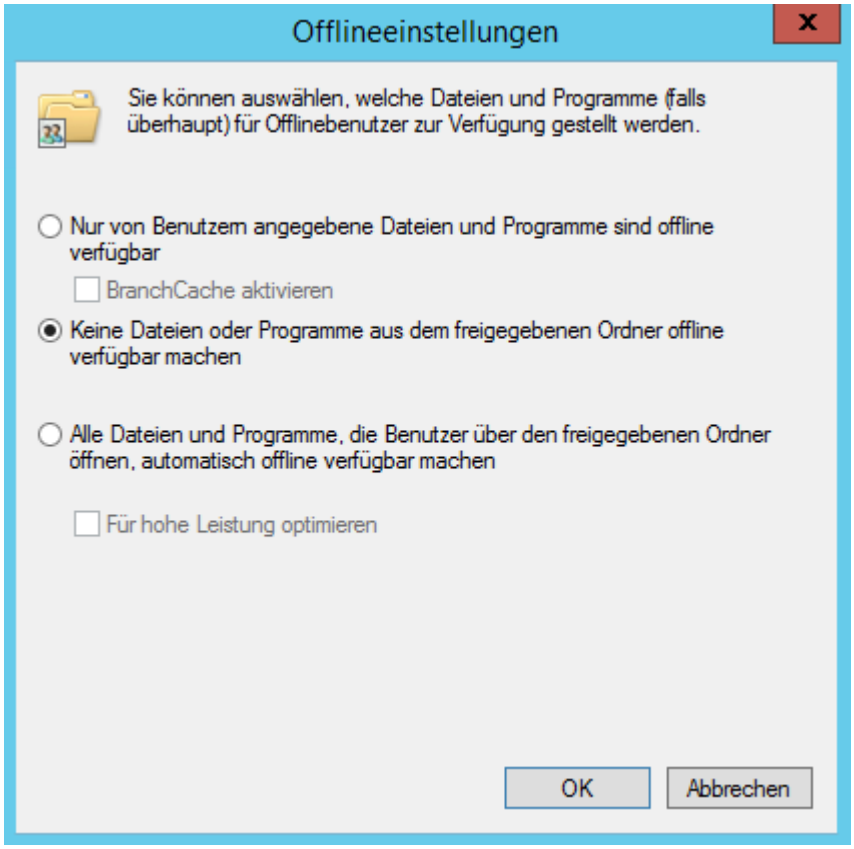
Probieren Sie das bitte von jedem Rechner aus, welcher auf die TSE zugreifen muss.

Hyper-V oder VMware etc.

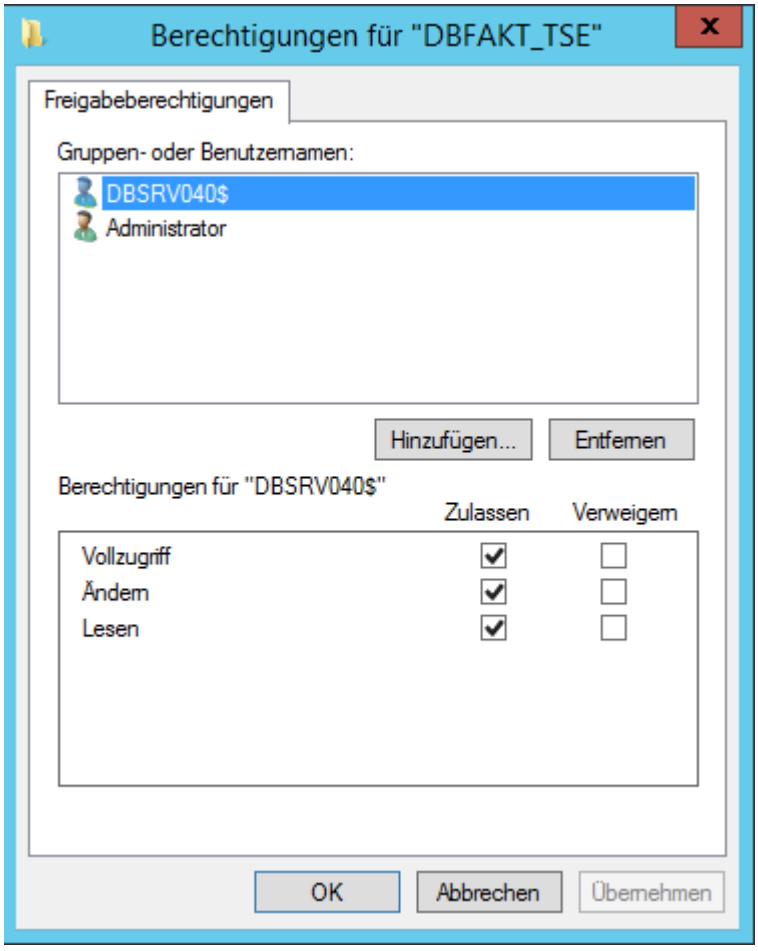
Bei Serverumgebungen mit Hyper-V bitte die TSE als Laufwerk freigeben:



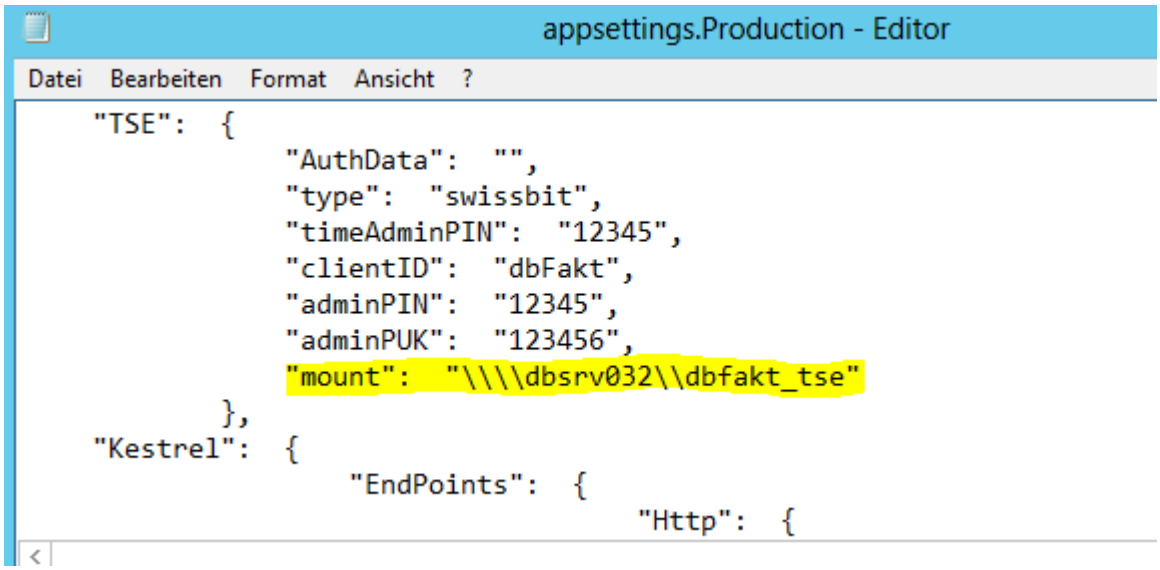
Bitte bei „Zwischenspeichern“ die Auswahl „Keine Dateien oder Programme aus dem freigegebenen Ordner offline verfügbar machen“ bei der nachfolgenden Einstellung setzen.



Bitte bei den Berechtigungen das Gerätekonto der virtuellen Maschine mit Vollzugriff erlauben:

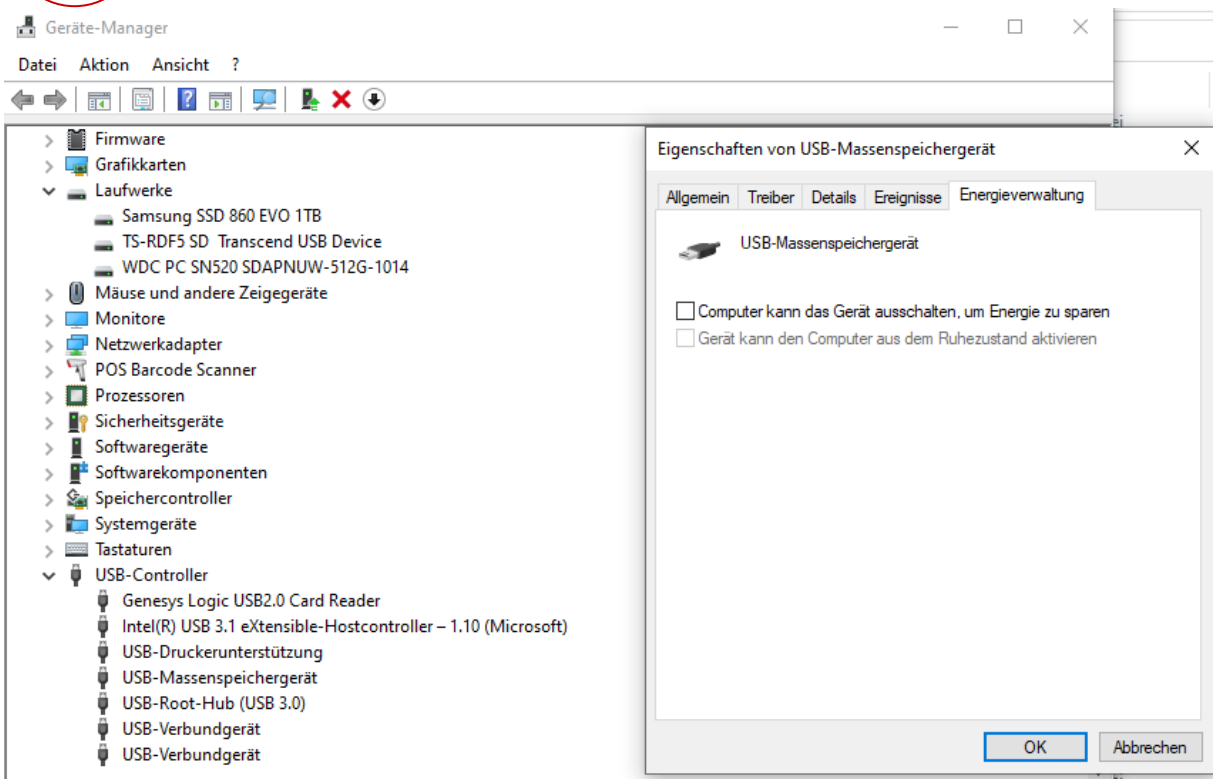


Es kann dann noch hilfreich sein in der „appsettings.Production.json“ nach der Config den Eintrag des Laufwerks „mount“ auf einen UNC Pfad abzuändern:



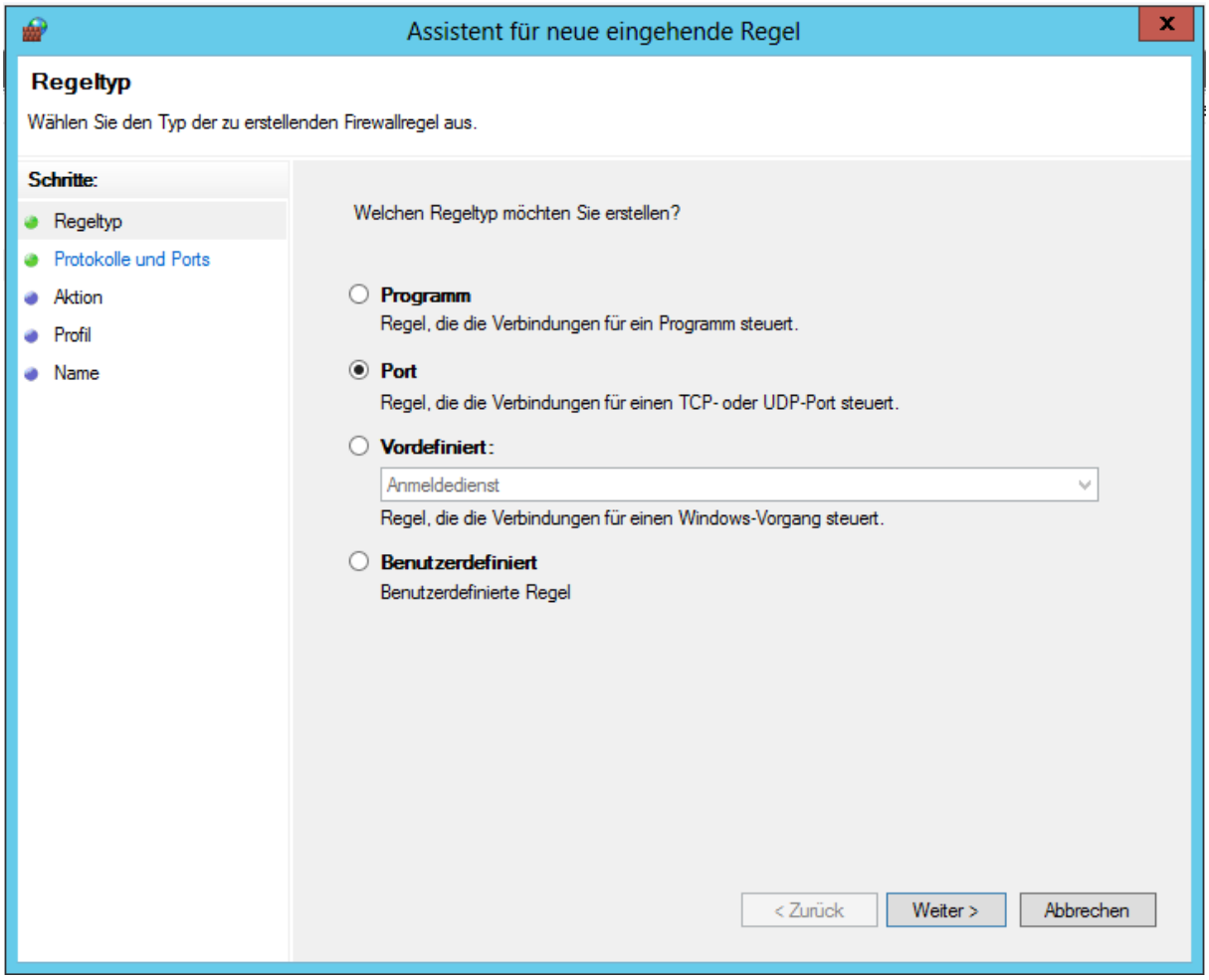
Energieverwaltung bei USB ausschalten

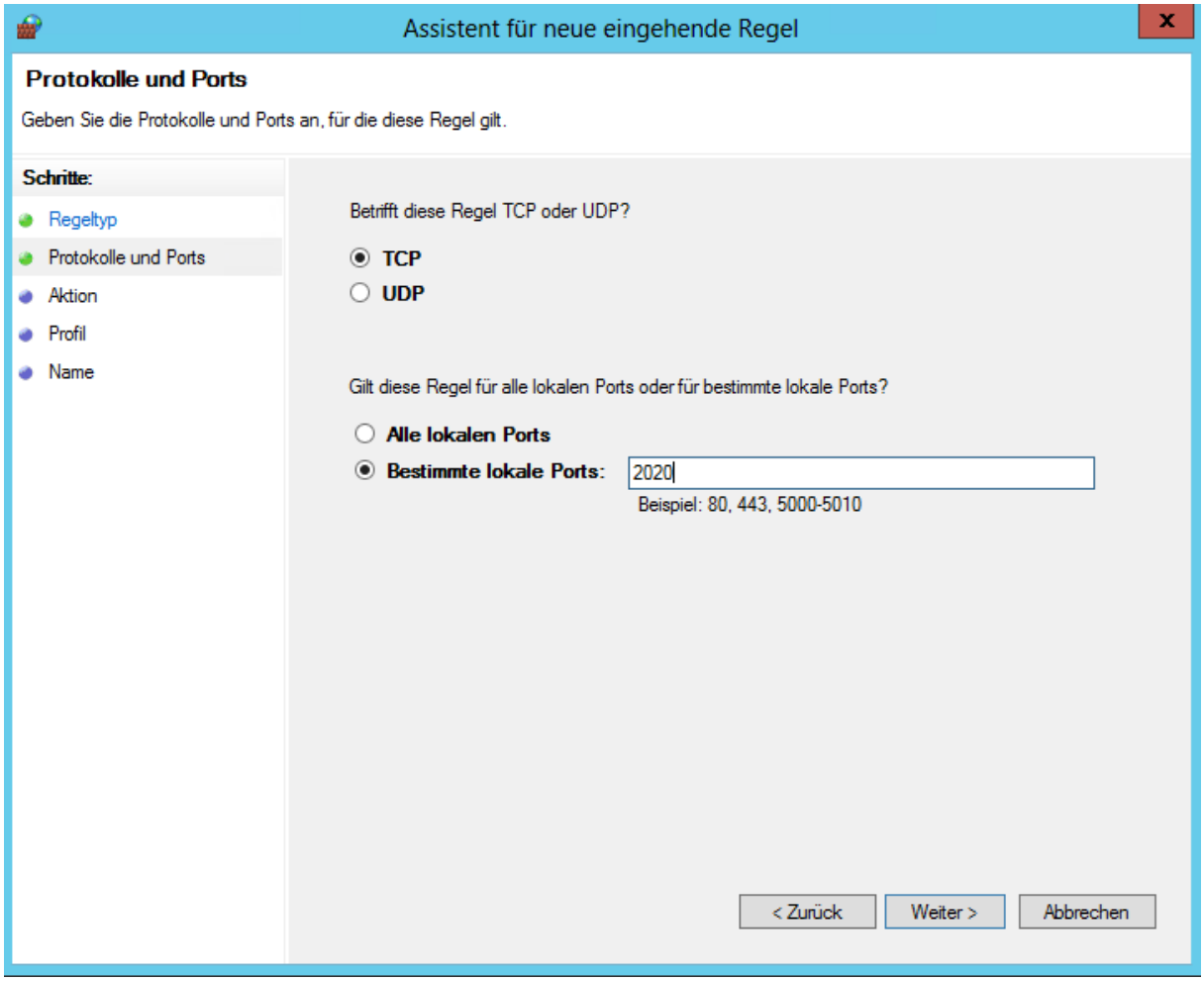
Bitte deaktivieren Sie die Einstellung für die Energiesparoption bei dem USB Port.

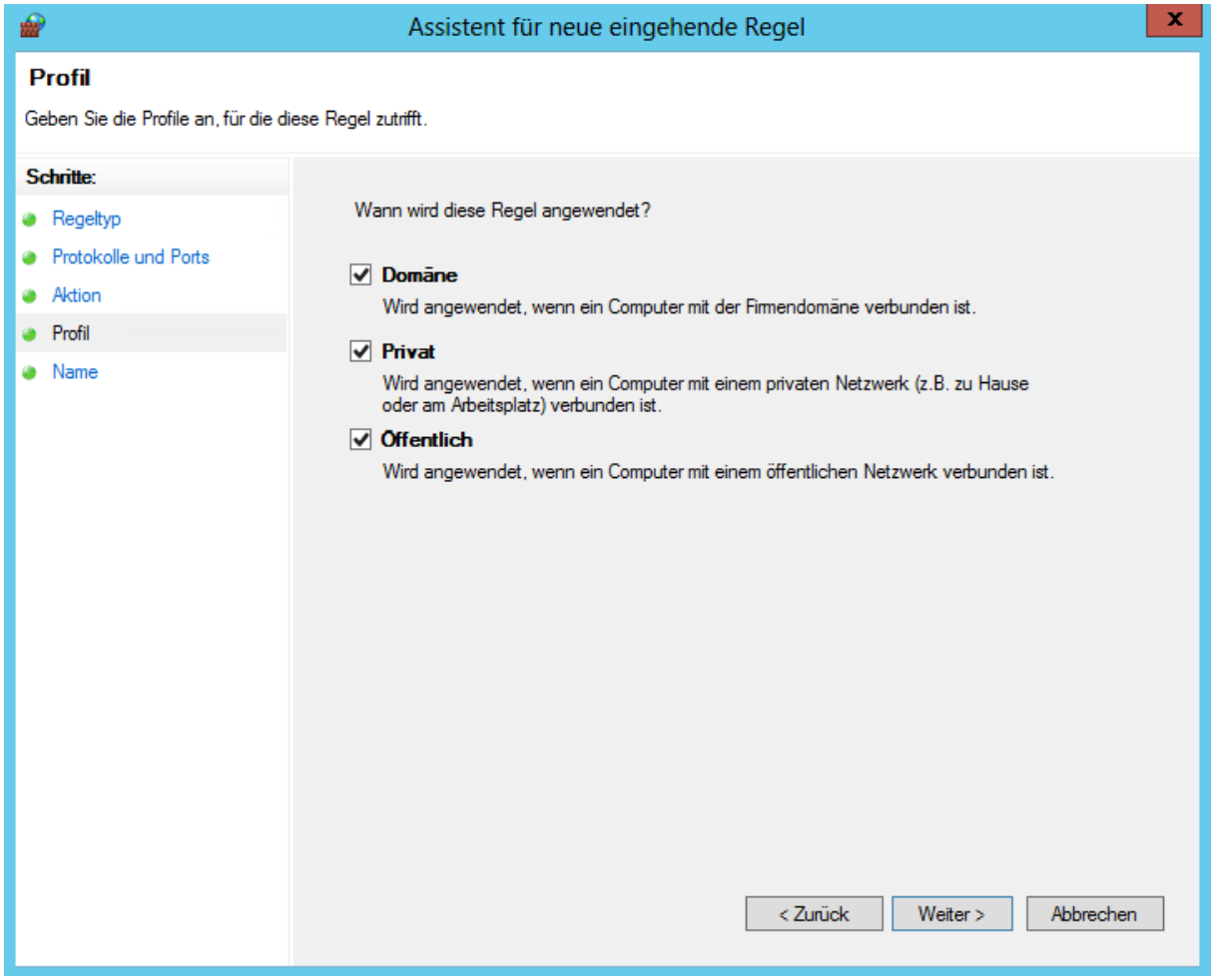


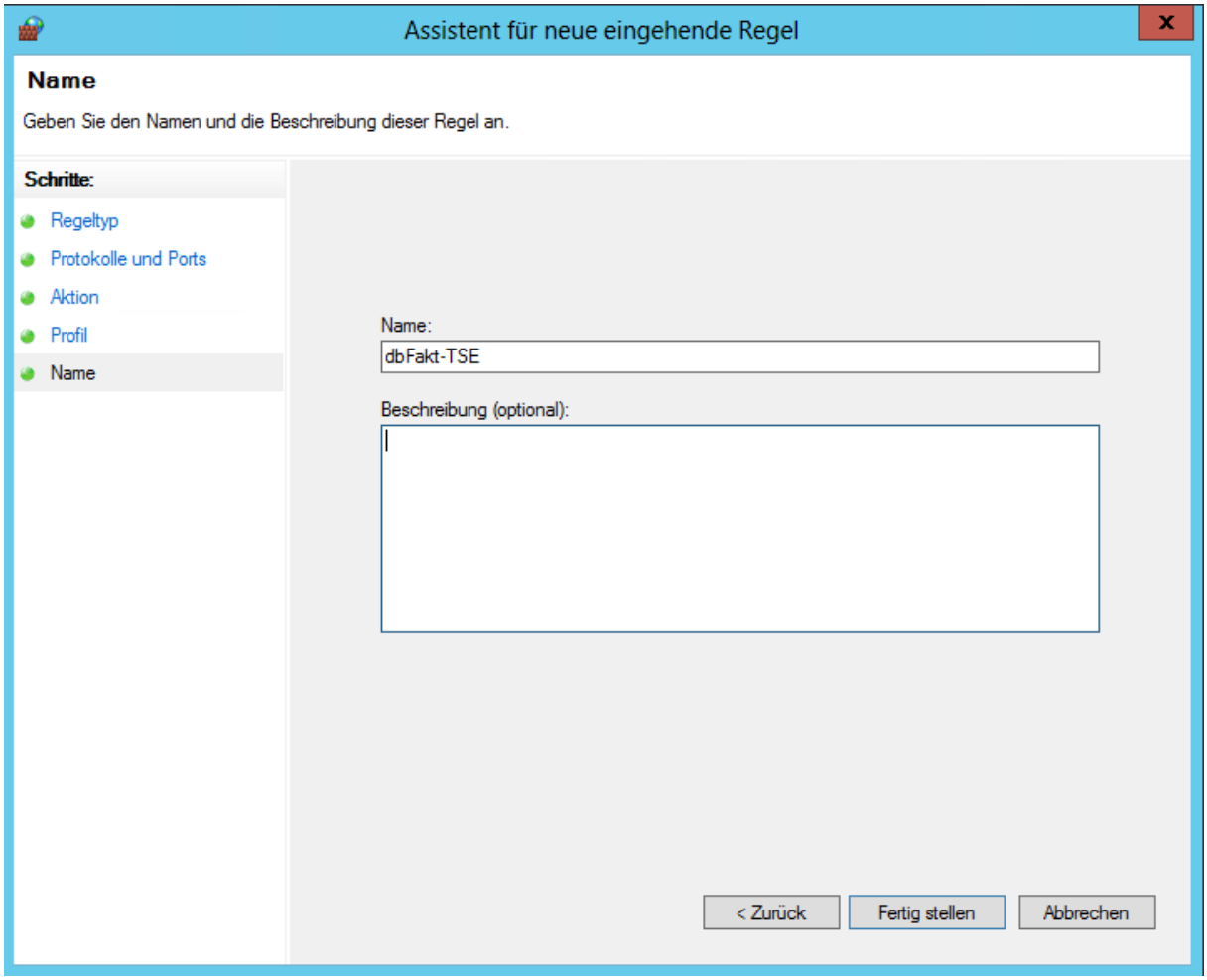
Einstellungen der Firewall

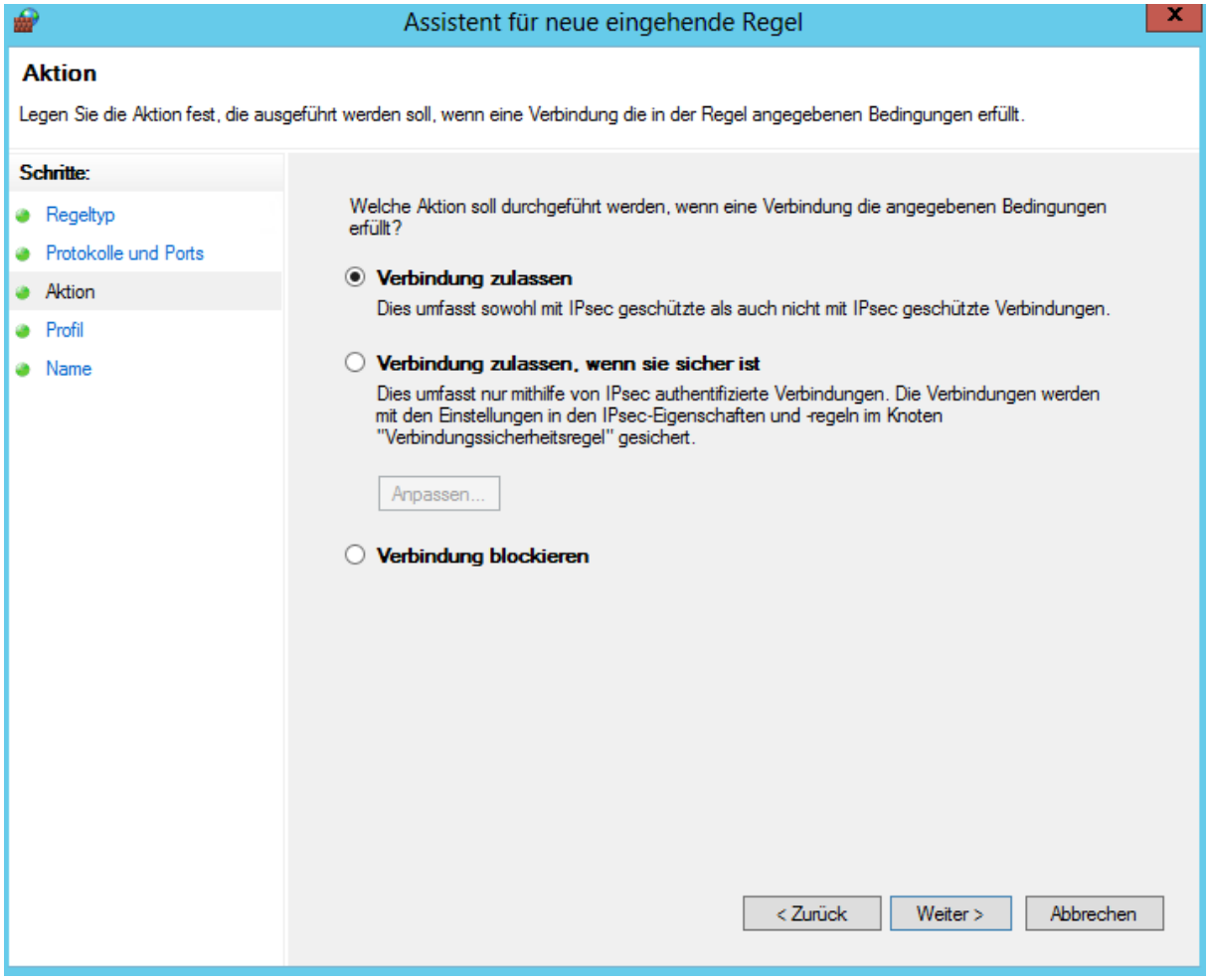
Wenn Sie von Clients nicht auf die TSE via Browser zugreifen können, dann sollten Sie auf dem Host noch eine Portfreigabe der Firewall konfigurieren:


Assistent für neue eingehende Regel
Regeltyp
Wählen Sie den Typ der zu erstellenden Firewallregel aus.
Schritte:
Regeltyp
Protokolle und Ports
Aktion
Profil
Name
Welchen Regeltyp möchten Sie erstellen?
Programm
Regel, die die Verbindungen für ein Programm steuert.
Port
Regel, die die Verbindungen für einen TCP- oder UDP-Port steuert.
Vordefiniert:
Anmeldedienst
Regel, die die Verbindungen für einen Windows-Vorgang steuert.
Benutzerdefiniert
Benutzerdefinierte Regel
< Zurück
Weiter >
Abbrechen


Assistent für neue eingehende Regel
Protokolle und Ports
Geben Sie die Protokolle und Ports an, für die diese Regel gilt.
Schritte:
Regeltyp
Protokolle und Ports
Aktion
Profil
Name
Betrifft diese Regel TCP oder UDP?
TCP
UDP
Gilt diese Regel für alle lokalen Ports oder für bestimmte lokale Ports?
Alle lokalen Ports
Bestimmte lokale Ports:
2020
Beispiel: 80, 443, 5000-5010
< Zurück
Weiter >
Abbrechen


Assistent für neue eingehende Regel
Profil
Geben Sie die Profile an, für die diese Regel zutrifft.
Schritte:
Regeltyp
Protokolle und Ports
Aktion
Profil
Name
Wann wird diese Regel angewendet?
Domäne
Wird angewendet, wenn ein Computer mit der Firmendomäne verbunden ist.
Privat
Wird angewendet, wenn ein Computer mit einem privaten Netzwerk (z.B. zu Hause oder am Arbeitsplatz) verbunden ist.
Öffentlich
Wird angewendet, wenn ein Computer mit einem öffentlichen Netzwerk verbunden ist.
< Zurück
Weiter >
Abbrechen


Assistent für neue eingehende Regel
Name
Geben Sie den Namen und die Beschreibung dieser Regel an.
Schritte:
Regeltyp
Protokolle und Ports
Aktion
Profil
Name
Name:
dbFakt-TSE
Beschreibung (optional):
< Zurück
Fertig stellen
Abbrechen


Assistent für neue eingehende Regel
Aktion
Legen Sie die Aktion fest, die ausgeführt werden soll, wenn eine Verbindung die in der Regel angegebenen Bedingungen erfüllt.
Schritte:
Regeltyp
Protokolle und Ports
Aktion
Profil
Name
Welche Aktion soll durchgeführt werden, wenn eine Verbindung die angegebenen Bedingungen erfüllt?
Verbindung zulassen
Dies umfasst sowohl mit IPsec geschützte als auch nicht mit IPsec geschützte Verbindungen.
Verbindung zulassen, wenn sie sicher ist
Dies umfasst nur mithilfe von IPsec authentifizierte Verbindungen. Die Verbindungen werden mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.
Anpassen...
Verbindung blockieren
< Zurück
Weiter >
Abbrechen